

KASPERSKY LAB

Kaspersky Mobile Security 7.0

BENUTZERHANDBUCH

KASPERSKY MOBILE SECURITY 7.0

Benutzerhandbuch

© Kaspersky Lab

www.kaspersky.de

Inhalt

KAPITEL 1. KASPERSKY MOBILE SECURITY 7.0	5
1.1. Hardware- und Software-Voraussetzungen	6
1.2. Bezugsadresse	6
KAPITEL 2. KASPERSKY MOBILE SECURITY FÜR SYMBIAN OS	7
2.1. Installation von Kaspersky Mobile Security	7
2.2. Bedienung	8
2.2.1. Programmaktivierung	8
2.2.2. Start des Programms	9
2.2.3. Grafische Oberfläche	10
2.2.4. Allgemeine Einstellungen	11
2.2.5. Viren-Suche und -Schutz	12
2.2.5.1. Echtzeitschutz und Scan auf Befehl	12
2.2.5.2. Untersuchung nach Zeitplan	16
2.2.6. Isolieren in Quarantäne	16
2.2.7. Module Anti-Spam und Diebstahlschutz (Anti-Theft)	18
2.2.7.1. Anti-Spam	19
2.2.7.2. „Schwarze“ und „weiße“ Liste bearbeiten	19
2.2.7.3. Anti-Spam-Einstellungen	21
2.2.7.4. Aktionen für Nachrichten	22
2.2.7.5. Diebstahlschutz (Anti-Theft)	23
2.2.7.6. Konfiguration von SMS-Clean	24
2.2.7.7. Konfiguration von SIM-Watch	25
2.2.8. Update der Programm-Datenbanken	26
2.2.8.1. Update-Einstellung	27
2.2.8.2. Manuelles Update	29
2.2.8.3. Update nach Zeitplan	29
2.2.9. Firewall	29
2.2.10. Ereignisprotokoll	30
2.3. Deinstallation der Anwendung	31

KAPITEL 3. KASPERSKY MOBILE SECURITY FÜR MICROSOFT WINDOWS MOBILE	33
3.1. Installation von Kaspersky Mobile Security.....	33
3.2. Erste Schritte.....	34
3.2.1. Programmaktivierung.....	34
3.2.2. Start des Programms	35
3.2.3. Grafische Oberfläche	36
3.3. Viren-Suche und -Schutz.....	38
3.3.1. Echtzeitschutz und Scan auf Befehl	38
3.3.2. Untersuchung nach Zeitplan.....	42
3.4. Isolieren in Quarantäne	43
3.5. Module Anti-Spam und Diebstahlschutz (Anti-Theft)	44
3.5.1. Anti-Spam.....	44
3.5.2. „Schwarze“ und „Weiße“ Liste bearbeiten.....	45
3.5.3. Aktionen für Nachrichten.....	46
3.5.4. Diebstahlschutz (Anti-Theft).....	47
3.5.4.1. Konfiguration von SMS-Clean	49
3.5.4.2. Konfiguration von SIM-Watch.....	50
3.6. Update der Programm-Datenbanken	51
3.7. Firewall	53
3.8. Ereignisprotokoll.....	54
3.9. Deinstallation der Anwendung.....	55
 ANHANG A. KASPERSKY LAB.....	 59
A.1. Kontaktinformationen.....	60
 ANHANG B. ENDBENUTZER-LIZENZVERTRAG FÜR DIE ERWORBENE KASPERSKY LAB SOFTWARE	 61

KAPITEL 1. KASPERSKY MOBILE SECURITY 7.0

Kaspersky Mobile Security 7.0 dient zum Schutz von Smartphones und Communicators mit den Betriebssystemen Symbian OS und Windows Mobile vor schädlichen Programmen und unerwünschten Nachrichten und übernimmt die folgenden Funktionen:

- **Echtzeitschutz** für das Dateisystem des Gerätes – Abfangen und Untersuchen aller
 - eingehenden Objekte, die über drahtlose Verbindungen empfangen werden (Infrarot-Port, Bluetooth), EMS- und MMS-Nachrichten, bei der Synchronisierung mit dem Personalcomputer und beim Aufrufen von Dateien über den Browser
 - Dateien, die sich auf dem mobilen Gerät öffnen lassen
 - Programme, die sich auf der Oberfläche des Gerätes installieren lassen
- **Untersuchung von Objekten** des Dateisystems, die sich auf dem mobilen Gerät oder angeschlossenen Speichererweiterungskarten befinden, auf Befehl des Benutzers und nach einem Zeitplan
- **Zuverlässiges Isolieren von infizierten Objekten** in eine Quarantäne
- **Update der Datenbanken von Kaspersky Mobile Security**, die zur Suche nach schädlichen Programmen und zum Löschen von gefährlichen Objekten eingesetzt werden
- **Sperren von unerwünschten SMS- und MMS-Nachrichten**
- **Sperren des Zugriffs oder Löschen von Benutzerdaten** bei nicht autorisierten Aktionen am Gerät, zum Beispiel bei Diebstahl
- **Schutz des Smartphones auf Netzwerkebene**

Dem Benutzer wird die Möglichkeit eingeräumt, die Einstellungen von Kaspersky Mobile Security flexibel zu verwalten, den aktuellen Status des Viren-Schutzes anzuzeigen und ein Ereignisjournal zu führen, in dem die Aktionen des Programms stehen.

Das Programm stellt eine einfach zu bedienende Benutzeroberfläche bereit.

Anmerkung

Sollte Kaspersky Mobile Security ein schädliches Programm erkennen, kann das infizierte Objekt desinfiziert (falls eine Desinfektion möglich ist), gelöscht oder in die Quarantäne verschoben werden. Eine Kopie wird vom zu löschenden Objekt nicht angelegt.

1.1. Hardware- und Software-Voraussetzungen

Kaspersky Mobile Security wird auf Smartphones und Communicators installiert, die mit den folgenden Betriebssystemen arbeiten:

- Symbian OS 9.1, 9.2 Series 60 UI
- Microsoft Windows Mobile 5.0
- Microsoft Windows Mobile 6.0

1.2. Bezugsadresse

Kaspersky Mobile Security kann über das Internet bezogen werden (Programm und Dokumentation in elektronischer Form):

www.kaspersky.de/store

KAPITEL 2. KASPERSKY MOBILE SECURITY FÜR SYMBIAN OS

In diesem Kapitel wird die Funktionsweise von Kaspersky Mobile Security 7.0 für Smartphones beschrieben, die unter dem Betriebssystem Symbian 9.1, 9.2 Series 60 UI laufen.

2.1. Installation von Kaspersky Mobile Security

Um Kaspersky Mobile Security zu installieren, machen Sie Folgendes:

- .1 Kopieren Sie die Programmdateien auf das Smartphone.
- .2 Rufen Sie das Setup auf (Programmdatei auf dem Smartphone öffnen).
- .3 Zur Bestätigung des Setups wählen Sie **Ja** (s. Abb. 1).



Abbildung 1. Setup-Nachfrage

- .4 Sollten die Sprachversionen vom Betriebssystem und von Kaspersky Mobile Security nicht zusammenpassen, erscheint eine entsprechende Meldung. Um das Setup in Deutsch fortzusetzen, klicken Sie auf **OK**.
- .5 Bitte lesen Sie sich die Lizenzvereinbarung durch. Wenn Sie den Punkten in der Vereinbarung zustimmen, klicken Sie auf **OK**. Um das Setup zu beenden, klicken Sie auf **Abbrechen** (s. Abb. 2).



Abbildung 2. Lizenzvereinbarung

Achtung!

Von Kaspersky Mobile Security kann kein funktionsfähiges Backup angelegt werden. Sollten es irgendwann einmal zu einer Beschädigung der Programmdateien kommen, empfehlen wir eine Neuinstallation.

2.2. Bedienung

In diesem Abschnitt erfahren Sie Näheres zum Einstellen der Parameter für den Viren-Scan auf Befehl und den Echtzeitschutz, für das Filtern von SMS- und MMS-Nachrichten, für das Updaten des Programms, den Schutz des Smartphones auf Netzwerkebene u.ä.

2.2.1. Programmaktivierung

Beim ersten Start des Programms erscheint auf dem Smartphone das Fenster für die Aktivierung von Kaspersky Mobile Security (s. Abb. 3).



Abbildung 3. Aktivierungsfenster des Programms

Das Programm muss aktiviert werden, sonst stehen die Funktionen von Kaspersky Mobile Security nicht zur Verfügung. Den Aktivierungscode bekommen Sie nach dem Kauf im Online-Shop per E-Mail zugeschickt.

Achtung!

Zur Aktivierung von Kaspersky Mobile Security auf dem Smartphone ist eine Internet-Verbindung erforderlich.

Der Aktivierungscode besteht aus Buchstaben des lateinischen Alphabets und Ziffern. Geben Sie die Code-Abschnitte nacheinander in die 4 Felder ein und achten Sie dabei auf Groß- und Kleinschreibung.

Nach Eingabe des Aktivierungscodes gehen Sie auf **Aktivieren** im Menü **Optionen**. Das Programm führt eine http-Anfrage an den Aktivierungsserver von Kaspersky Lab durch, lädt den Lizenzschlüssel herunter und installiert ihn.

Wenn der von Ihnen eingegebene Aktivierungscode aus irgendeinem Grund nicht gültig ist, erscheint auf dem Smartphone eine entsprechende Meldung.

2.2.2. Start des Programms

Um Kaspersky Mobile Security zu starten, gehen Sie wie folgt vor:

- 1 Öffnen Sie das Hauptmenü des Smartphones.
- 2 Gehen Sie auf das Symbol **KMS 7.0** und starten Sie das Programm, indem Sie den Punkt **Öffnen** im Menü **Optionen** auswählen.

Anmerkung

Beim ersten Start des Programms wird Ihnen vorgeschlagen, die Funktion **Auto-start** zu aktivieren (s. Pkt. 2.2.4 auf S. 11). Klicken Sie auf **OK**, falls Sie dies wünschen.

Nach dem Start erscheint auf dem Display des Smartphones das Fenster für den Status der Basiskomponenten von Kaspersky Mobile Security (s. Abb. 4):

- **Echtzeitschutz** – Status des Echtzeitschutzes (s. Pkt. 2.2.5 auf S. 12)
- **Letzte Untersuchung** – Datum der letzten Viren-Suche
- **Datenbanken vom** – Datum der Antiviren -Datenbanken
- **Anti-Spam** – Funktionsmodus für Anti-Spam (s. Pkt. 2.2.7 auf S. 18)
- **Firewall-Stufe** – Schutzstufe des Smartphones (s. Pkt. 2.2.9 auf S. 29)



Abbildung 4. Fenster Status der Programmkomponenten

Um zur eigentlichen Programmoberfläche zu wechseln, klicken Sie auf **OK**.

2.2.3. Grafische Oberfläche

Die grafische Oberfläche des Programms besteht aus sechs Registerkarten:

- Auf der Registerkarte **Untersuchung** können Sie einen Viren-Scan starten die Parameter dafür einstellen, den Echtzeitschutz-Modus bearbeiten und einen Zeitplan für den Start einer automatischen Untersuchung konfigurieren.
- Auf der Registerkarte **Quarantäne** verwalten Sie die Quarantäne, eine spezielle Ablage für infizierte und verdächtige Objekte.
- Auf der Registerkarte **Update** können Sie Updates der Antiviren-Datenbanken durchführen, die Parameter für Updates bearbeiten und einen Zeitplan für Updates konfigurieren.
- Die Registerkarte **Firewall** kontrolliert die Netzwerkaktivität und den Schutz des Smartphones auf Netzwerkebene.
- Auf der Registerkarte **Sonstiges** stellen Sie die Filter-Parameter für eingehende SMS- und MMS-Nachrichten (Modul Anti-Spam) ein, sperren das Smartphone und löschen Daten bei einem Diebstahl des Gerätes (Modul Diebstahlschutz).
- Auf der Registerkarte **Informationen** können Sie das Ereignisjournal für die Programmkomponenten und allgemeine Informationen zum Programm und der verwendeten Datenbanken anzeigen sowie die allgemeinen Parameter für die Programmfunktionen bearbeiten.

Zum Navigieren zwischen den Registerkarten verwenden Sie die Navigationstasten des Smartphones (Richtungstasten bzw. kleiner Joystick) oder gehen Sie im Menü **Optionen** auf den Punkt **Registerkarte öffnen** (s. Abb. 5).



Abbildung 5. Menü **Funktionen**

Um zum Fenster mit dem Status der Programmkomponenten zurückzukehren, gehen Sie auf den Punkt **Aktueller Status** im Menü **Optionen**.

2.2.4. Allgemeine Einstellungen

Die auf der Registerkarte **Informationen** im Punkt **Einstellungen** (s. Abb. 6) befindlichen Parameter sorgen für die folgenden Programmfunktionen:

- **Autostart** – Funktionsmodus für Autostart. Im aktiven Autostart-Modus werden die Grundfunktionen des Programms beim Einschalten des Smartphones gestartet. Durch das Deaktivieren von Autostart werden die Grundfunktionen beendet. Wählen Sie **Ja** aus, wenn Sie wollen, dass die Grundfunktionen immer Ihr Smartphone schützen sollen.
- **Statusfenster zeigen** bestimmt, ob der aktuelle Status beim Programmstart angezeigt werden soll.
- **Protokollgröße** bestimmt die höchstens zulässige Größe der Protokoll-Datei. Wird der Grenzwert erreicht, werden alte Protokollmeldungen gelöscht.
- **Hintergrundlicht** bestimmt, ob die Hintergrundbeleuchtung bei der Viren-Suche eingeschaltet bleiben soll. Als Standard ist die Hintergrundbeleuchtung deaktiviert.
- **Ton bei Virenfund** bestimmt die Sound-Benachrichtigung bei Eintreten von bestimmten Ereignissen (Erkennen eines infizierten Objektes, Meldungen zum Programmstatus usw.). Wählen Sie **Ja** aus, wenn Sie einen Sound hören wollen.
- **Vibration** bestimmt, ob das Smartphone beim Erkennen eines infizierten Objektes vibrieren soll. In der Grundeinstellung ist die Vibration aktiviert.

Abbildung 6. Menü **Einstellungen**

Zum Bearbeiten der Werte benutzen Sie die Navigations-Tasten des Smartphones oder gehen Sie im Menü **Optionen** auf den Punkt **Ändern**.

2.2.5. Viren-Suche und -Schutz

Auf der Registerkarte **Untersuchung** können Sie einen Viren-Scan des gesamten Dateisystems und Smartphone-Speichers oder einzelner Verzeichnisse bzw. Dateien starten. Außerdem können Sie die Parameter für die Viren-Suche und den Echtzeitschutz-Modus ändern, das Protokoll über die Suchergebnisse anzeigen und einen Zeitplan für den automatischen Start einer Untersuchung einrichten.

2.2.5.1. Echtzeitschutz und Scan auf Befehl

Der Echtzeitschutz ist ein Modus, bei dem ein Teil von Kaspersky Mobile Security dauerhaft im Arbeitsspeicher des Smartphones liegt und alle Daten wie den Posteingang (von außen zum Smartphone gelangende Nachrichten) kontrolliert.

Der Echtzeitschutz ist mit dem Einschalten des Smartphones in Betrieb und funktioniert bis zum Ausschalten (wenn dieser Modus nicht in den Einstellungen deaktiviert wurde).

Kaspersky Mobile Security kann das Dateisystem des Smartphones komplett untersuchen und dabei Objekte analysieren, die sich auf eingesteckten Speicher-Erweiterungskarten befinden.

Die Ergebnisse des Echtzeitschutzes und des Scans auf Befehl werden in einen Bericht eingetragen. Zum Anzeigen des Berichts wählen Sie auf der Registerkarte **Untersuchung** den Eintrag **Protokoll**.

Um den Echtzeitschutz zu starten, machen Sie Folgendes:

- 1 Auf der Registerkarte **Untersuchung** gehen Sie auf **Einstellungen**.

- .2 Aktivieren / Deaktivieren Sie den Echtzeitschutz, indem Sie den entsprechenden Wert bei **Echtzeitschutz** setzen.

Um die Parameter für einen Scan auf Befehl zu ändern, machen Sie Folgendes:

- .1 Auf der Registerkarte **Untersuchung** gehen Sie auf **Einstellungen**.
- .2 Geben Sie im Block **Dateityp** den Untersuchungsbereich ein, indem Sie die Dateitypen markieren, die untersucht werden sollen:
 - **Alle Dateien** – Es werden alle Dateien untersucht.
 - **Ausführbare** – Untersucht werden nur ausführbare Programmdateien (zum Beispiel *.exe, *.sis, *.mdl, *.app).
- .3 Wählen Sie die Aktion beim Erkennen eines infizierten Objektes (Parameter **Aktion/Virus**).

Wenn Sie wollen, dass beim Erkennen eines infizierten Objektes das Smartphone den Benutzer nach einer Aktion fragt, setzen Sie den Wert auf **Aktion erfragen**.

Zum automatischen Löschen ohne Benachrichtigung des Benutzers setzen Sie den Wert auf **Löschen**.

Zum automatischen Verschieben von erkannten Objekten in die Quarantäne setzen Sie den Wert auf **Quarantäne**. Das Verschieben eines infizierten Objektes in die Quarantäne ist eine standardmäßig ausgeführte Aktion.

- .4 Aktivieren / Deaktivieren Sie die Untersuchung des ROM-Speichers für das Smartphone (Parameter **ROM-Untersuchung**).

Unter bestimmten Umständen kann der ROM-Speicher für schädliche Programme anfällig sein. Damit Kaspersky Mobile Security diesen Speicher untersuchen kann, setzen Sie den Wert auf **Ja**.

- .5 Aktivieren / Deaktivieren Sie das Entpacken von SIS- und ZIP-Archiven (Parameter **Archive entpacken**).

Damit Kaspersky Mobile Security bei einer Untersuchung SIS- und ZIP-Archive entpackt, setzen Sie den Wert auf **Ja**. Wenn ein Entpacken von Archiven nicht gebraucht wird, deaktivieren Sie diese Funktion, indem Sie sie auf **Nein** setzen.

- .6 Aktivieren / Deaktivieren Sie den Modus zur Untersuchung einer neuen Karte (Parameter **Neue Karten scannen**).

Damit Kaspersky Mobile Security in das Smartphone eingesteckte Flash-Karten untersuchen kann, setzen Sie den Wert auf **Untersuchung**. Um die automatische Untersuchung von Flash-Karten zu deaktivieren, wählen Sie **Deaktiviert** aus. Damit Kaspersky Mobile Security

jedes Mal beim Einstecken einer neuen Karte nachfragt, setzen Sie den Wert auf **Aktion erfragen**.

- .7 Aktivieren / Deaktivieren Sie die Darstellung des Schutzsymbols (Parameter **Schutz-Symbol**).

Damit bei aktiviertem Echtzeitschutz das Programmsymbol auf dem Smartphone angezeigt wird, setzen Sie den Wert im entsprechenden Menüpunkt auf **Immer**. Wenn Sie wollen, dass das Symbol nur im Menü des Smartphones angezeigt wird, setzen Sie den Wert auf **Nur im Menü**. Damit das Symbol nicht angezeigt wird, setzen Sie den Wert auf **Nie**.

Anmerkung

Zum Bearbeiten des Wertes benutzen Sie die Navigations-Tasten des Smartphones oder gehen Sie im Menü **Optionen** auf den Punkt **Ändern**.

Das Programm arbeitet standardmäßig mit Einstellungen, die von den Kaspersky-Lab-Experten empfohlen werden. Wenn Sie im Laufe der Arbeit mit dem Programm zu den empfohlenen Einstellungen zurückkehren wollen, öffnen Sie die Registerkarte **Untersuchung** und gehen im Menü **Optionen** auf den Punkt **Wiederherstellen**.

Um eine Viren-Suche zu starten, machen Sie Folgendes:

- .1 Starten Sie Kaspersky Mobile Security (s. Pkt. 2.2.2 auf S. 9).
- .2 Auf der Registerkarte **Untersuchung** (s. Abb. 7) wählen Sie den Punkt **Alles untersuchen**, wenn Sie das gesamte Dateisystem des Smartphones untersuchen wollen, oder **Ordner scannen**, wenn Sie einen einzelnen Ordner untersuchen wollen.



Abbildung 7. Registerkarte **Untersuchung**

Nach Auswahl des Punktes **Ordner scannen** sehen Sie das Dateisystem des Smartphones. Um die Untersuchung eines Ordners zu starten, setzen Sie den Cursor auf den Ordner und gehen auf den Punkt **Untersuchen** im Menü **Optionen**.

Nachdem die Untersuchung begonnen hat, öffnet sich das Untersuchungsfenster, in dem der aktuelle Status angezeigt wird: Anzahl der untersuchten Objekte, Pfad zu einem Objekt, das gerade untersucht wird, und Fortschrittsanzeige in Prozent (s. Abb. 8).

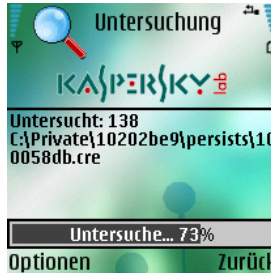


Abbildung 8. Untersuchungsfenster

Sollte ein infiziertes Objekt erkannt werden, werden Sie gefragt, ob Sie die infizierte Datei löschen wollen (Aktion **Löschen**), ob sie es in die Quarantäne verschieben wollen (Aktion **In die Quarantäne**), oder ob Sie die Datei unverändert lassen wollen (Aktion **Überspringen**).

Achtung!

Das Programm fragt die Aktion für ein Objekt nur dann nach, wenn der Untersuchungsparameter **Aktion** den Wert **Aktion erfragen** (Details s. Pkt. 2.2.5.1 auf S. 12) hat.

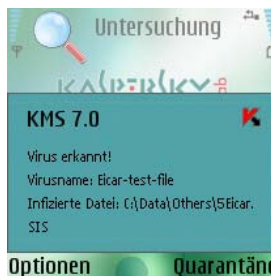


Abbildung 9. Meldung eines erkannten Virus

Nach der Untersuchung erscheint eine allgemeine Statistik über gefundene und gelöschte schädliche Objekte.

Damit die Hintergrundbeleuchtung während der Untersuchung nicht ausgeschaltet wird, wechseln Sie zur Registerkarte **Informationen**, öffnen Sie das Menü **Einstellungen** und setzen Sie den Wert **Ja** für den Parameter **Hintergrundlicht**. Wenn Sie die Tastatur des Smartphones nicht bedienen, wird

standardmäßig die Hintergrundbeleuchtung automatisch ausgeschaltet, um Batterieladung zu sparen.

2.2.5.2. Untersuchung nach Zeitplan

Mit Kaspersky Mobile Security kann der Benutzer einen Zeitplan für das automatische Untersuchen des Smartphones erstellen. Die Untersuchung erfolgt im Hintergrund. Wenn ein infiziertes Objekt erkannt wird, wird die Aktion ausgeführt, die in den Sucheinstellungen vorgegeben wurde (s. Pkt. 2.2.5.1 auf S. 12).

Die Untersuchung nach Zeitplan ist standardmäßig deaktiviert.

Um eine Untersuchung nach Zeitplan einzurichten, machen Sie Folgendes:

Auf der Registerkarte **Untersuchung** gehen Sie auf den Punkt **Zeitplan** und richten die Parameter **Startmodus** ein (s. Abb. 10):

- **Täglich** – Untersuchung erfolgt jeden Tag. Im Eingabefeld geben Sie die **Zeit** ein.
- **Wöchentlich** – Untersuchung erfolgt einmal pro Woche. Geben Sie den **Tag** und die **Zeit** ein.



Abbildung 10. Menü **Zeitplan**

2.2.6. Isolieren in Quarantäne

Infizierte Objekte, die in die Quarantäne verschoben wurden, bedrohen nicht mehr die Sicherheit des Smartphones und können später gelöscht oder wiederhergestellt werden.

Als infiziert erkannte Objekte können von der Anwendung automatisch oder nach Ihrer Bestätigung in die Quarantäne verschoben werden.

Damit die Anwendung automatisch infizierte Objekte in die Quarantäne verschiebt, wechseln Sie zur Registerkarte **Untersuchung**, wählen Sie den

Punkt **Einstellungen** und setzen Sie den Wert **Quarantäne** für den Parameter **Aktion**.

Falls Sie **Aktion erfragen** angegeben haben, schlägt Ihnen Kaspersky Mobile Security beim Erkennen eines infizierten Objektes vor, das Objekt zu löschen oder es in die Quarantäne zu verschieben.

Auf die Grundfunktionen der Quarantäne greifen Sie über die Registerkarte **Quarantäne** zu (s. Abb. 11).



Abbildung 11. Menü **Quarantäne**

Wählen Sie **Quarantäne** aus, um die Liste mit allen Objekten anzuzeigen, die in der Quarantäne liegen (s. Abb. 12).



Abbildung 12. Infizierte Objekte in der Quarantäne

Im Menü **Optionen**, das im Quarantäne-Fenster angeboten wird, können Sie Folgendes machen:

- Detaillierte Informationen zu jedem Objekt anzeigen, das in der Quarantäne gespeichert wird (**Hinweise**)
- Aktuelles Objekt löschen (**Löschen**)
- Quarantäne leeren, indem der gesamte Inhalt mit den Objekten gelöscht wird (**Alle löschen**)

- Aktuelles Objekt aus der Quarantäne in ursprüngliches Verzeichnis wiederherstellen (**Wiederherstellen**)
- Hilfe anfordern (**Hilfe**)

Um die Parameter für die Quarantäne einzurichten, gehen Sie in das Menü **Einstellungen**, das sich auf der Registerkarte **Quarantäne** befindet (s. Abb. 13).



Abbildung 13. Quarantäne einrichten

Der Parameter **Quarantäne-Größe** bestimmt die maximale Anzahl von infizierten Objekten, die in der Quarantäne gespeichert werden können. Sie können als mögliche Werte **20**, **50** oder **100** Dateien eingeben.

Der Parameter **Speicherdauer** bestimmt die Dauer, die die infizierten Objekte in der Quarantäne gespeichert bleiben können. Nach Ablauf der eingegebenen Frist werden die infizierten Objekte automatisch gelöscht.

Anmerkung

Um die Einstellungen der Quarantäne wiederherzustellen, die die Kaspersky-Lab-Experten empfohlen haben, wählen Sie im Menü **Optionen** den Punkt **Wiederherstellen**.

2.2.7. Module Anti-Spam und Diebstahlschutz (Anti-Theft)

Das Modul Anti-Spam schützt das Smartphone vor unerwünschten SMS- und MMS-Nachrichten.

Das Filter-Prinzip für Nachrichten beruht auf der Verwendung einer „schwarzen“ und einer „weißen“ Liste (Blacklist und Whitelist). Nachrichten, die von Telefonnummern eingehen, die auf einer „schwarzen“ Liste stehen, werden von Anti-Spam gesperrt. Nachrichten von Telefonnummern, die auf einer „weißen“ Liste stehen, werden nicht gesperrt.

Das Modul Diebstahlschutz sperrt das Smartphone und löscht bei einem Diebstahl oder Verlust des Gerätes Daten im Speicher.

2.2.7.1. Anti-Spam

Um den Anti-Spam-Modus einzurichten, wechseln Sie auf die Registerkarte **Sonstiges**, gehen Sie auf den Punkt **Anti-Spam** und dann auf **Einstellungen**. Bestimmen Sie einen der folgenden Modi mit dem Parameter **Anti-Spam**:

- **Aktiviert.** In diesem Modus filtert Anti-Spam eingehende Nachrichten anhand der „schwarzen“ und „weißen“ Liste. Geht eine Nachricht von einer Telefonnummer ein, die in keiner Liste steht, warnt Anti-Spam den Benutzer und schlägt das Sperren oder Zulassen des Nachrichteneingangs vor und empfiehlt außerdem die Übernahme der Telefonnummer in die „weiße“ oder „schwarze“ Liste.
- **Nur Listen.** In diesem Modus filtert Anti-Spam eingehende Nachrichten nur anhand von Daten, die in der „schwarzen“ und „weißen“ Liste stehen. Nachrichten von Nummern, die auf keiner Liste stehen, werden ohne Nachfrage beim Benutzer zugelassen.
- **Deaktiviert.** In diesem Modus ist Anti-Spam deaktiviert. Eingehende Nachrichten werden nicht gefiltert.

2.2.7.2. „Schwarze“ und „weiße“ Liste bearbeiten

Die „schwarze Liste“ und die „weiße Liste“ enthalten Einträge mit Telefonnummern, von denen der Empfang von SMS- und/oder MMS-Nachrichten durch Anti-Spam gesperrt oder freigegeben ist. Die Daten zu gesperrten und gelöschten Nachrichten stehen im Abschnitt **Protokoll**.

Anmerkung

Nachrichten, die auf keiner Liste stehen, werden beim Empfang nicht gesperrt!

Um die „schwarze“ oder „weiße“ Liste zu bearbeiten, wechseln Sie auf die Registerkarte **Anti-Spam** (s. Abb. 14) und gehen Sie auf die entsprechende Liste.

Abbildung 14. Menü **Anti-Spam**

Zur Bearbeitung der Liste gehen Sie auf das Menü **Optionen**:

- **Eintrag hinzufügen** – Es wird ein neuer Eintrag in der Liste erzeugt.
- **Eintrag bearbeiten** – Der aktuelle Eintrag wird bearbeitet.
- **Eintrag löschen** – Der aktuelle Eintrag wird gelöscht.
- **Alle Einträge löschen** – Die Liste wird geleert, indem alle Einträge gelöscht werden.
- **Hilfe** – Hilfe für die Listenfunktionen

Entscheiden Sie sich für den Punkt **Eintrag hinzufügen** oder **Eintrag bearbeiten**, werden Ihnen die folgenden Parameter für den Eintrag vorgeschlagen:

- **Nachrichtenart.** Geben Sie an, welche Arten eingehender Nachrichten gesperrt (für „schwarze“ Liste) oder zugelassen (für „weiße“ Liste) werden sollen. Mögliche Werte: **Nur SMS**, **Nur MMS** und **Alle Nachrichten**.
- **Tel.-Nr.** Geben Sie die Telefonnummer an, für die der Nachrichtempfang gesperrt oder zugelassen ist. Die Nummer kann mit einer Ziffer oder dem Zeichen „+“ beginnen und darf nur Ziffern enthalten. Außerdem dürfen beim Anlegen der Nummer die Ersatzzeichen „?“ (steht für eine einzelne Ziffer) und „*“ (steht für eine beliebig lange Ziffernfolge) verwendet werden.
- Im Feld **Text** tragen Sie einen Text ein, bei dessen Erkennen durch das Programm in der eingegangenen Nachricht die folgenden Aktionen ausgeführt werden:
 - Die Nachricht, in der Text gefunden wird, der in der "weißen" Liste steht, wird übersprungen.
 - Die Nachricht, in der Text gefunden wird, der in der "schwarzen" Liste steht, wird gesperrt.

Die Analyse der Nachricht erfolgt in dieser Reihenfolge:

- Untersuchung der Nummer auf Zugehörigkeit zur "schwarzen" Liste
- Untersuchung der Nummer auf Zugehörigkeit zur "weißen" Liste
- Untersuchung des Nachrichtentextes danach, was in der "schwarzen" Liste steht
- Untersuchung des Nachrichtentextes danach, was in der "weißen" Liste steht

Wenn die Nachricht zu einer Regel passt, erfolgt die weitere Untersuchung und die Nachricht wird übersprungen oder gesperrt, je nach der Zugehörigkeit zur "schwarzen" oder "weißen" Liste.

Nach dem Setzen der Parameter klicken Sie auf **Zurück**, um den Eintrag zu speichern und zum Fenster mit der Listenanzeige zu wechseln (s. Abb. 15).



Abbildung 15. „Schwarze“ Liste

2.2.7.3. Anti-Spam-Einstellungen

Um Anti-Spam einzurichten, wechseln Sie auf die Registerkarte **Anti-Spam** und gehen auf den Punkt **Einstellungen** (s. Abb. 16).



Abbildung 16. Anti-Spam-Einstellungen

Im Menü **Einstellungen** lassen sich die folgenden Parameter für Anti-Spam bearbeiten:

- **Kontakte zulassen:** Wenn der Parameter den Wert **Ja** hat, sperrt Anti-Spam niemals den Nachrichtenempfang von Telefonnummern, die in Ihrem Telefonbuch gespeichert sind. Wenn diese Option deaktiviert ist (Wert steht auf **Nein**), richtet sich Anti-Spam beim Filtern danach, ob die Telefonnummer in der „schwarzen“ oder „weißen“ Liste steht.
- **Postausgang hinzu.** Wenn der Parameter den Wert **Ja** hat, werden alle Telefonnummern, denen Sie eine SMS- oder MMS-Nachricht senden, automatisch in die „weiße“ Liste gespeichert. Zum Deaktivieren dieser Option wählen Sie **Nein** aus.
- **Nicht-Ziffern sperren:** Wenn der Parameter den Wert **Nein** hat, sperrt Anti-Spam den Nachrichtenempfang von Nicht-Ziffer-Nummern nicht. Zum Aktivieren dieser Option wählen Sie **Ja** aus.
- **Arten unterscheiden.** Wenn der Parameter den Wert **Nein** hat, wird für neue Einträge, die Anti-Spam in der „weißen“ oder „schwarzen“ Liste erstellt, als Nachrichtenart der Wert **Alle Nachrichten** (Details zu Einträgen in Listen s. Pkt. 2.2.7.2 auf S. 19) hinterlegt, sonst werden Einträge für bestimmte Nachrichtenarten (SMS oder MMS) erstellt.

Anmerkung

Dieser Parameter beeinflusst nur Einträge, die Anti-Spam in einer der folgenden Situationen erstellt hat:

- Erfassen von ausgehenden Nummern in der „weißen“ Liste (Parameter **Postausgang hinzu** aktiviert)
- Erfassen von neuen Telefonnummern in einer Liste, von denen eine Nachricht eingegangen ist (s. Pkt. 2.2.7.4 auf S. 22)

2.2.7.4. Aktionen für Nachrichten

Geht eine SMS- oder MMS-Nachricht von einer Telefonnummer ein, die nicht in der „schwarzen“ oder „weißen“ Liste steht, fängt sie das Anti-Spam-Modul ab und meldet den Vorgang (s. Abb. 17).



Abbildung 17. Spam-Warnung

Über das Menü **Optionen** können Sie eine der folgenden Aktionen für eine Nachricht wählen:

- **In „weiße“ Liste** – Empfang der Nachricht wird zugelassen und die Telefonnummer des Absenders in der „weißen“ Liste gespeichert.
- **In „schwarze“ Liste** – Empfang der Nachricht wird gesperrt und die Telefonnummer des Absenders in der „schwarzen“ Liste gespeichert.
- **Überspringen** – Empfang der Nachrichten wird zugelassen, die Telefonnummer des Absenders in keine Liste gespeichert.

Wenn in den Anti-Spam-Einstellungen für den Parameter **Arten unterscheiden** der Wert **Nein** gesetzt ist, wird bei der gewählten Aktion **In „weiße“ Liste** oder **In „schwarze“ Liste** in der jeweiligen Liste ein Eintrag für alle Nachrichtenarten erstellt (**Nachrichtenart – Alle Nachrichten**), sonst richtet sich der Typ nach der empfangenen Nachricht (Details über die Parameter für Listen-Einträge s. Pkt. 2.2.7.2 auf S. 19).

Die Daten über gesperrte Nachrichten werden in das Anwendungsprotokoll eingetragen. Zum Anzeigen des Berichtes müssen Sie auf der Registerkarte **Sonstiges** den Eintrag **Protokoll** wählen.

2.2.7.5. Diebstahlschutz (Anti-Theft)

Das Modul schützt Daten, die auf dem mobilen Gerät gespeichert sind, vor dem unautorisierten Zugriff, falls das Gerät gestohlen wird oder verloren geht.

Beim erstmaligen Aufruf der Modul-Einstellungen müssen Sie einen Geheimcode definieren. Mit dessen Hilfe können Sie künftig auf die Modul-Einstellungen zugreifen, um sie zu ändern. Der Geheimcode wird gebraucht, damit die Einstellungen nicht unautorisiert geändert werden können und damit der Benutzer Daten sperren und löschen kann, die auf dem Smartphone bei Diebstahl oder Verlust gespeichert waren.

Die Funktion **SMS-Block** sperrt das Gerät auf Wunsch des Benutzers. Es lässt sich erst nach Eingabe eines Geheimcodes entsperren, der für den Zugriff auf das Diebstahlschutz-Modul verwendet wird. Die Einstellung tritt in Kraft, nachdem der Benutzer, dem das Smartphone gestohlen wurde, an das gestohlene Gerät die SMS **block:Code** (also **block:** direkt gefolgt von dem entsprechenden Code) sendet. Um diese Option zu verwenden, gehen Sie auf **Aktiviert**.

Die Funktion **SMS-Clean** löscht persönliche Benutzerdaten (Kontakte, Nachrichten, Galerie). Die Einstellung tritt in Kraft, nachdem der Benutzer, dem das Gerät gestohlen wurde, an das gestohlene Gerät die SMS **clean:Code** (also **clean:** direkt gefolgt von dem entsprechenden Code) sendet. Um **SMS-Clean** zu verwenden, gehen Sie auf **Aktiviert**.

Die Funktion **SIM-Watch** sendet beim Wechsel der SIM-Karte auf einem gestohlenen Smartphone die neue Telefonnummer an die angegebenen Nummern und sperrt das Gerät. Um diese Option zu verwenden, gehen Sie auf **Aktiviert**.

Wenn der Geheimcode für das Diebstahlschutz-Modul geändert werden muss, gehen Sie auf den Punkt **Code ändern**. Geben Sie den neuen Code ein, wiederholen Sie ihn zur Sicherheit nochmal und klicken Sie auf **OK**.

Bei jedem Zugriff auf die Einstellungen des Moduls Diebstahlschutz (s. Abb. 18) muss der vorgegebene Geheimcode eingegeben werden.



Abbildung 18. Registerkarte **Diebstahlschutz**

Die vorgenommenen Aktionen werden in das Anwendungsprotokoll eingetragen. Zum Anzeigen des Berichtes wählen Sie auf der Registerkarte **Sonstiges** den Eintrag **Protokoll**.

2.2.7.6. Konfiguration von SMS-Clean

Um **SMS-Clean** einzurichten, wechseln Sie auf die Registerkarte **Sonstiges** und gehen auf den Punkt **Diebstahlschutz**. Geben Sie den Geheimcode

(s. Pkt. 2.2.7.5 auf S. 23) ein und gehen Sie im nächsten Fenster auf den Punkt **SMS-Clean**.

Der Abschnitt **SMS-Clean** enthält eine Liste von Daten, die gelöscht werden sollen, wenn das Smartphone gestohlen wird oder verloren geht (s. Abb. 19).



Abbildung 19. Registerkarte **SMS-Clean**

Wenn Sie wollen, dass bei einem Verlust des mobilen Gerätes oder dessen Diebstahl das Telefonbuch gelöscht wird, gehen Sie auf den Punkt **Kontakte löschen** und setzen Sie den Wert auf **Ja**.

Zum Löschen von Post, SMS- und MMS-Nachrichten (Ordner Inbox und Mailbox) gehen Sie auf den Punkt **Nachrichten löschen** und setzen Sie den Wert auf **Ja**.

Der Punkt **Galerie leeren** löscht persönliche Daten (Daten aus dem Ordner !:\Data\). Standardmäßig ist das Löschen von persönlichen Daten nicht vorgesehen. Wenn Sie wollen, dass bei einem Diebstahl oder Verlust des Smartphones die persönlichen Daten gelöscht werden können, gehen Sie auf diesen Punkt und setzen Sie den Wert auf **Ja**.

Klicken Sie auf **OK**, um die vorgenommenen Änderungen zu speichern.

2.2.7.7. Konfiguration von SIM-Watch

Um SIM-Watch einzurichten, wechseln Sie auf die Registerkarte **Sonstiges** und gehen Sie auf den Punkt **Diebstahlschutz**. Geben Sie den Geheimcode (s. Pkt. 2.2.7.5 auf S. 23) ein und gehen Sie im nächsten Fenster auf den Punkt **SIM Watch**.

Das Modul **SIM Watch** überwacht den Wechsel der SIM-Karte auf dem Gerät (s. Abb. 20).

Abbildung 20. Registerkarte **SIM Watch**

In den Feldern **Telefonnummer 1** und **Telefonnummer 2** geben Sie diejenigen Telefonnummern ein, an die Sie die neue Telefonnummer erhalten wollen, falls die SIM-Karte auf Ihrem Smartphone gewechselt wird. Die Nummern können mit einer Ziffer oder dem Zeichen „+“ beginnen und dürfen nur Ziffern enthalten.

Zusätzlich können Sie eine Sperre des Smartphones beim Wechsel der SIM-Karte einrichten. Gehen Sie dazu auf den Punkt **Telefon sperren** und setzen Sie den Wert auf **Ja**. Das Gerät wird mit Eingabe des Geheimcodes entsperrt, der für den Zugriff auf das Diebstahlschutz-Modul angegeben wurde. Standardmäßig ist das Sperren des Gerätes nicht vorgesehen.

Klicken Sie auf **OK**, um die vorgenommenen Änderungen zu speichern.

2.2.8. Update der Programm-Datenbanken

Nach schädlichen Programmen wird mithilfe von Einträgen in einer Programm-Datenbank gesucht, in der eine Beschreibung aller bekannten und zurzeit als schädlich eingestuften Programme steht. Es ist absolut wichtig, dass die Datenbanken stets auf dem neuesten Stand sind.

Die Datenbanken können entweder manuell oder automatisiert nach Zeitplan aktualisiert werden. Das Update erfolgt über das Internet von den Kaspersky-Lab-Servern.

Sie können die automatische Viren-Untersuchung des Smartphones nach jedem Update der Datenbanken von Kaspersky Mobile Security aktivieren. Wechseln Sie dazu auf die Registerkarte **Update**, gehen Sie auf den Punkt **Einstellungen** und setzen Sie im Punkt **Scan nach Update** den Wert auf **Aktiviert**.

Die Option **Quarantäne n. Update** bestimmt, ob die Objekte in der Quarantäne jedes Mal nach dem Update der Programm-Datenbanken untersucht werden sollen oder nicht. Standardmäßig erfolgt diese Untersuchung. Um eine Untersuchung zu unterbinden, wählen Sie **Deaktiviert** aus.

Wenn Sie nicht jedes Mal beim Update einen Access Point im Internet auswählen wollen, setzen Sie den Parameter **Access Point auswählen** auf den Wert **Nein**, so dass sich das Programm den letzten Access Point merkt, über den das Update erfolgreich gelaufen ist, und diesen künftig als Netzverbindung zugrunde legt. Zudem können Sie einen neuen Access Point angeben.

Soll der aktive Access Point geändert werden, verwenden Sie den Parameter **Access Point**. Sie müssen dann den gewünschten Parameterwert in der Liste auswählen. Standardmäßig ist der Access Point der Default-Wert des Gerätes.

Der Punkt **Update-Server** bestimmt die Quelle für das Update der Programm-Datenbanken: entweder der Update-Server von Kaspersky Lab (Wert **Standard**) oder ein vom Benutzer angegebener Server (Wert **Eingeben**). Bei Auswahl des Wertes **Eingeben** tragen Sie im nächsten Fenster die URL eines Update-Servers ein. Bei Bedarf kann ein alternativer Update-Server eingegeben werden.

Detaillierte Informationen zu den gerade verwendeten Datenbanken finden Sie unter dem Punkt **Datenbank-Info**, der sich auf der Registerkarte **Informationen** befindet.

Der Update-Vorgang der Datenbanken wird in das Protokoll eingetragen. Um das Protokoll anzuzeigen, gehen Sie auf der Registerkarte **Update** auf den Punkt **Protokoll**.

2.2.8.1. Update-Einstellung

Um das Update für die Programm-Datenbanken einzurichten, machen Sie Folgendes:

- .1 Starten Sie Kaspersky Mobile Security (s. Pkt. 2.2.2 auf S. 9).
- .2 Auf der Registerkarte **Update** gehen Sie auf den Punkt **Einstellungen** (s. Abb. 21).



Abbildung 21. Registerkarte **Update**

- .3 Aktivieren / Deaktivieren Sie die Frage nach dem Access Point (Option **Access Point auswählen**).

Anmerkung

Der Access Point wird mit Parametern eingerichtet, die der Mobilfunkbetreiber vorschreibt.

Wenn Sie sich für **Nein** entscheiden, erfolgt die Verbindung über den Access Point, der beim letzten Update verwendet wurde.

Bei der Auswahl von **Ja** schlägt das Programm vor, den Access Point aus einer Liste von verfügbaren Access Points auszuwählen (s. Abb. 22).



Abbildung 22. Access Point auswählen

- 4 Geben Sie die Adresse des Update-Servers (wenn nötig) ein. Gehen Sie dazu auf den Punkt **Update-Server** und setzen Sie den Wert auf **Eingeben**. Im nächsten Fenster geben Sie die URL eines Update-Servers ein (s. Abb. 23).

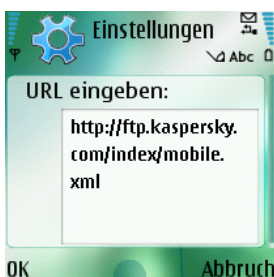


Abbildung 23. Adresse des Update-Servers

Standardmäßig erfolgen Updates vom Kaspersky-Lab-Server <http://ftp.kaspersky.com/index/mobile.xml>.

Achtung!

Unabhängig davon, ob bereits zuvor eine Internetverbindung bestand, wird sie nach dem Update-Vorgang geschlossen.

2.2.8.2. Manuelles Update

Um das Update von Hand aufzurufen, machen Sie Folgendes:

- .1 Starten Sie Kaspersky Mobile Security (s. Pkt. 2.2.2 auf S. 9).
- .2 Auf der Registerkarte **Update** gehen Sie auf den Punkt **Update** (s. Abb. 21).

2.2.8.3. Update nach Zeitplan

Um das Update der Datenbanken nach Zeitplan einzurichten, machen Sie Folgendes:

- .1 Starten Sie Kaspersky Mobile Security (s. Pkt. 2.2.2 auf S. 9).
- .2 Auf der Registerkarte **Update** gehen Sie auf den Punkt **Zeitplan** und wählen einen Modus für **Auto-Update**:
 - **Deaktiviert** – kein Update nach Zeitplan durchführen
 - **Täglich** – Update erfolgt jeden Tag. Geben Sie die Update-Uhrzeit in das entsprechende Feld ein.
 - **Wöchentlich** – Update erfolgt einmal pro Woche. Geben Sie den Update-Tag und die Update-Uhrzeit in die entsprechenden Felder ein.

2.2.9. Firewall

Die Firewall kontrolliert die Netzwerkaktivität und den Schutz des Smartphones auf Netzwerkebene (s. Abb. 24).

Sie können die Schutzstufe der **Firewall anpassen**. Um eine Überwachungsstufe für den ein- und ausgehenden Traffic festzulegen, können Sie unter den vorgeschlagenen Varianten auswählen:

- **Alle blockieren** - Jede Netzwerkaktivität wird unterbunden.
- **Mittel** - Alle eingehenden Verbindungen werden gesperrt. Ausgehende Verbindungen können nur über die Standard-Anwendungen erfolgen.

- **Niedrig** - Es werden nur eingehende Verbindungen gesperrt.
- **Deaktiviert** - Jegliche Netzwerkaktivität wird zugelassen.

Mit dem Parameter **Benachrichtigung** können Sie Benachrichtigungen für den Benutzer einrichten, wenn seine Aktionen nicht der eingestellten Sicherheitsstufe entsprechen. Um den Empfang von Benachrichtigungen zu unterbinden, wählen Sie **Deaktiviert** aus.



Abbildung 24. Registerkarte **Firewall**

Die Ereignisse des Firewall-Moduls werden in das Anwendungsprotokoll eingetragen. Zum Anzeigen des Berichtes wählen Sie auf der Registerkarte **Firewall** den Eintrag **Protokoll**.

2.2.10. Ereignisprotokoll

Auf der Registerkarte **Informationen** können Sie das chronologische Ereignisprotokoll für Kaspersky Mobile Security anzeigen lassen. Wechseln Sie dazu auf die Registerkarte und gehen Sie auf den Punkt **Protokoll** (s. Abb. 25).



Abbildung 25. Ereignisprotokoll

2.3. Deinstallation der Anwendung

Um Kaspersky Mobile Security vom Smartphone zu deinstallieren, gehen Sie wie folgt vor:

- .1 Beenden Sie Kaspersky Mobile Security. Machen Sie dazu Folgendes:
 - Klicken Sie auf **Menü** und halten Sie die Auswahlstaste gedrückt.
 - In der Liste der gestarteten Programme gehen Sie auf **KMS 7.0** und klicken auf die Schaltfläche **Optionen**.
 - Gehen Sie auf den Menüpunkt **Beenden** (s. Abb. 26).



Abbildung 26. Programm beenden

- .2 Deinstallieren Sie Kaspersky Mobile Security:
 - Klicken Sie auf die Schaltfläche **Menü** und gehen Sie auf den Menüpunkt **Progr.-Man.** (s. Abb. 27).



Abbildung 27. Programm-Manager starten

- In der Programmliste gehen Sie auf **KMS 7.0** und klicken auf die Schaltfläche **Optionen** (s. Abb. 28).



Abbildung 28. Programm auswählen

- Gehen Sie auf den Menüpunkt **Deinstallieren** (s. Abb. 29).

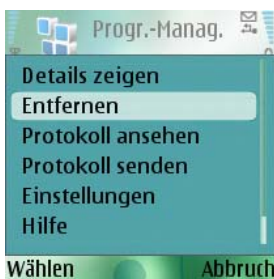


Abbildung 29. Deinstallation der Anwendung

- Zum Bestätigen der Programm-Deinstallation klicken Sie auf die Schaltfläche **Ja**.

KAPITEL 3. KASPERSKY MOBILE SECURITY FÜR MICROSOFT WINDOWS MOBILE

In diesem Kapitel wird die Funktionsweise von Kaspersky Mobile Security für mobile Geräte beschrieben, die mit einem der folgenden Betriebssysteme laufen:

- Microsoft Windows Mobile 5.0
- Microsoft Windows Mobile 6.0

Die Software ist nur für Smartphones und Communicators vorgesehen, die den Empfang und die Übermittlung von SMS-Nachrichten unterstützen.

3.1. Installation von Kaspersky Mobile Security

Um Kaspersky Mobile Security zu installieren, machen Sie Folgendes:

- .1 Kopieren Sie die CAB-Archivdatei von Kaspersky Mobile Security auf das mobile Gerät.
- .2 Rufen Sie das Setup auf (CAB-Archivdatei auf mobilem Gerät öffnen). Die Installation erfolgt in den Hauptspeicher des mobilen Gerätes.
- .3 Bitte lesen Sie sich die Lizenzvereinbarung durch. Wenn Sie den Punkten in der Vereinbarung zustimmen, klicken Sie auf **OK**. Um das Setup zu beenden, klicken Sie auf **Abbrechen** (s. Abb. 30).



Abbildung 30. Lizenzvereinbarung

3.2. Erste Schritte

Dieses Kapitel beschreibt die Programmaktivierung nach der Installation sowie den Programmstart. Außerdem erklärt es die Struktur der grafischen Benutzeroberfläche.

3.2.1. Programmaktivierung

Beim ersten Start des Programms erscheint auf dem Display des mobilen Gerätes das Fenster für die Aktivierung von Kaspersky Mobile Security (s. Abb. 31).



Abbildung 31. Fenster Aktivierung des Programms

Das Programm muss aktiviert werden, sonst stehen die Funktionen von Kaspersky Mobile Security nicht zur Verfügung. Den Aktivierungscode bekommen Sie nach dem Kauf im Online-Shop per E-Mail zugeschickt.

Achtung!

Zur Aktivierung von Kaspersky Mobile Security auf dem mobilen Gerät wird eine Internet-Verbindung gebraucht.

Der Aktivierungscode besteht aus Buchstaben des lateinischen Alphabets und Ziffern. Geben Sie die Code-Abschnitte nacheinander in die 4 Felder ein und achten Sie dabei auf Groß- und Kleinschreibung.

Nach Eingabe des Aktivierungscodes klicken Sie auf die Schaltfläche **Aktivierung**. Das Programm führt eine http-Anfrage an den Aktivierungsserver von Kaspersky Lab durch, lädt den Lizenzschlüssel herunter und installiert ihn.

Wenn der von Ihnen eingegebene Aktivierungscode aus irgendeinem Grund nicht gültig ist, erscheint auf dem Smartphone eine entsprechende Meldung.

3.2.2. Start des Programms


Um Kaspersky Mobile Security zu starten, machen Sie Folgendes:

- .1 Öffnen Sie auf dem mobilen Gerät das Menü **Programme**.
- .2 Gehen Sie auf den Punkt **KMS 7.0**, um das Programm zu starten.

Nach dem Start des Programms erscheint auf dem Display das Fenster für den Status der Basiskomponenten von Kaspersky Mobile Security (s. Abb. 32):

- **Echtzeitschutz** – Status des Echtzeitschutzes
- **Letzte Untersuchung** – Datum für die letzte Viren-Suche
- **Datenbanken von** – Datum der Antiviren -Datenbanken

Achtung!

Wenn das mobile Gerät nicht auf Viren untersucht wurde oder seit dem letzten Update der Antiviren-Datenbanken zwei Wochen vergangen sind, verändert das Symbol neben dem jeweiligen Punkt sein Aussehen in . Das gleiche Symbol erscheint, wenn der Echtzeitschutz und / oder das Anti-Spam-Modul deaktiviert werden.

- **Firewall** - Schutzstufe des Smartphones
- **Anti-Spam** – Status des Anti-Spam-Moduls zum Filtern von SMS-Nachrichten



Abbildung 32. Fenster Status der Programmkomponenten

3.2.3. Grafische Oberfläche

Die grafische Programmoberfläche besteht aus sechs Registerkarten, auf die Sie über den Punkt **Menü** zugreifen können (s. Abb. 33):

- Auf der Registerkarte **Untersuchung** können Sie einen Viren-Scan starten, die Parameter für die Viren-Suche und den Echtzeitschutz bearbeiten sowie einen Zeitplan für den Start einer automatischen Untersuchung konfigurieren (s. Pkt. 3.3 auf S. 38).
- Die Registerkarte **Firewall** kontrolliert die Netzwerkaktivität und den Schutz des Smartphones auf Netzwerkebene (s. Pkt. 2.2.9 auf S. 29).
- Auf der Registerkarte **Update** können Sie Updates der Antiviren-Datenbanken durchführen, die Parameter für Updates bearbeiten und einen Zeitplan für Updates konfigurieren (s. Pkt. 3.6 auf S. 51).
- Auf der Registerkarte **Quarantäne** können Sie die Quarantäne verwalten, eine spezielle Ablage für infizierte und verdächtige Objekte (s. Pkt. 3.4 auf S. 43).
- Auf der Registerkarte **Sonstiges** wird das Filtern der eingehenden SMS- und MMS-Nachrichten (Modul Anti-Spam) eingestellt, das Smartphone gesperrt und darauf gespeicherte Daten bei einem Diebstahl oder Verlust des Gerätes gelöscht (Modul Anti-Theft) (s. Pkt. 2.2.7.5 auf S. 23).
- Auf der Registerkarte **Informationen** können das Ereignisjournal für die Programmkomponenten, allgemeine Informationen zum Programm und der verwendeten Datenbanken angezeigt sowie die allgemeinen Parameter für die Programmfunktionen bearbeitet werden (s. Pkt. 3.8 auf S. 54).



Abbildung 33. Menü Programme

Um zum Status-Fenster zurückzukehren, gehen Sie auf den Punkt **Aktueller Status**.

Um das Programm zu beenden, gehen Sie auf **Beenden**.

3.3. Viren-Suche und -Schutz

Auf der Registerkarte **Untersuchung** können Sie einen Viren-Scan des gesamten Dateisystems und des Speichers für das mobile Gerät oder einzelner Verzeichnisse bzw. Dateien einstellen. Außerdem können Sie die Optionen für die Viren-Suche und den Echtzeitschutz ändern, das Protokoll über die Suchergebnisse anzeigen und einen Zeitplan für den automatischen Start einer Untersuchung einrichten.

3.3.1. Echtzeitschutz und Scan auf Befehl

Der Echtzeitschutz ist ein Modus, bei dem sich ein residenter Teil von Kaspersky Mobile Security dauerhaft im Hintergrund alle Aktivitäten auf dem mobilen Gerät schützt.

Der Echtzeitschutz ist mit dem Einschalten des Gerätes in Betrieb und funktioniert bis zum Ausschalten (wenn der Modus nicht in den Einstellungen deaktiviert wurde).

Außerdem kann Kaspersky Mobile Security das Dateisystem des mobilen Gerätes komplett untersuchen.

Die Ergebnisse des Echtzeitschutzes und des Scans auf Befehl werden in einen Bericht eingetragen. Zum Anzeigen des Berichtes wählen Sie den Eintrag **Untersuchungsbericht**. Außerdem erreichen Sie den Bericht auf der Registerkarte **Informationen** (s. Pkt. 3.8 auf S. 54).

Um den Echtzeitschutz zu starten, gehen Sie wie folgt vor:

- 1 Auf der Registerkarte **Untersuchung** gehen Sie auf **Scaneinstellungen**.
- 2 Aktivieren / Deaktivieren Sie den Echtzeitschutz, indem Sie das Häkchen von **Echtzeitschutz** setzen/entfernen.

Die Parameter für einen Scan auf Befehl ändern Sie wie folgt:

- 1 Auf der Registerkarte **Untersuchung** gehen Sie auf **Scaneinstellungen**.
- 2 Markieren Sie im Block **Parameter** die Dateitypen, die untersucht werden sollen:

- **Archive untersuchen** – Dateien untersuchen, die als Archiv gepackt sind
 - **Nur ausführbare** – Nur ausführbare Programm-Dateien untersuchen
- .3 Wählen Sie die Aktion aus, die das Programm bei Entdecken eines infizierten Objektes im Block **Bei Viruserkennung** ausführt. Damit Kaspersky Mobile Security versucht, ein erkanntes infiziertes Objekt zu desinfizieren, setzen Sie das Häkchen bei **Desinfektionsversuch**. Für den Fall, dass das Objekt nicht desinfiziert werden kann, können Sie über die Option **Wenn Desinfektion nicht geht** eine Alternativ-Aktion bestimmen:
- **In Quarantäne** – Die erkannten infizierten Objekte werden in die Quarantäne verschoben.
 - **Aktion erfragen** – Virenfunde werden gemeldet, der Benutzer hat dann die Wahl, das infizierte Objekt zu löschen, es in die Quarantäne zu verschieben oder zu überspringen.
 - **Löschen** – Erkannte infizierte Objekte werden gelöscht.
 - **Überspringen** – An infizierten Objekten werden keine Aktionen ausgeführt.

Außerdem können Sie eine der angeführten Aktionen für den Fall vorgeben, wenn der Desinfektionsversuch für ein infiziertes Objekt nicht gelungen ist. Setzen Sie dazu das Häkchen in **Desinfektionsversuch** und markieren Sie die gewünschte Aktion in der Liste **Wenn Desinfektion nicht geht**.

Um eine Viren-Suche zu starten, gehen Sie wie folgt vor:

- .1 Starten Sie Kaspersky Mobile Security (s. Pkt. 3.2.1 auf S. 34).
- .2 Wechseln Sie zur Registerkarte **Scaneinstellungen**.
 - Markieren Sie im Block **Parameter** die Dateitypen, die untersucht werden sollen (s. oben).
 - Wählen Sie die Aktion aus, die das Programm bei Entdecken eines infizierten Objektes ausführen soll (s. oben).
- .3 Auf der Registerkarte **Untersuchung** (s. Abb. 34) wählen Sie den Punkt **Alles untersuchen**, wenn Sie das gesamte Dateisystem des mobilen Gerätes untersuchen wollen, oder **Ordner untersuchen**, wenn Sie einen einzelnen Ordner untersuchen wollen.



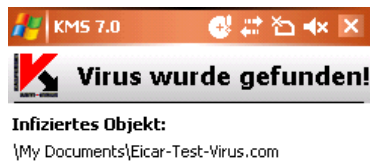
Abbildung 34. Registerkarte **Untersuchung**

Sollten Sie sich für den Punkt **Ordner untersuchen** entschieden haben, wird das Dateisystem des mobilen Gerätes angezeigt. Um die Untersuchung eines Ordners zu starten, setzen Sie den Cursor auf den Ordner und gehen auf **Untersuch..**

Nachdem die Suche begonnen hat, öffnet sich das Untersuchungsfenster, in dem der aktuelle Status angezeigt wird, mit der Anzahl der untersuchten Objekte und dem Pfad zum Objekt, das gerade untersucht wird (s. Abb. 35).



Abbildung 35. Untersuchungsfenster



Virusname:
Eicar-test-file



Abbildung 36. Meldung eines erkannten Virus

Nach der Untersuchung erscheint eine allgemeine Statistik über gefundene und gelöschte schädliche Objekte.

3.3.2. Untersuchung nach Zeitplan

Mit Kaspersky Mobile Security kann der Benutzer einen Zeitplan für die automatische Viren-Suche des mobilen Gerätes erstellen. Die Untersuchung erfolgt im Hintergrund. Wird ein infiziertes Objekt erkannt, wird die Aktion ausgeführt, die in den Sucheinstellungen vorgegeben wurde (Punkt **Scaneinstellungen**).

Die Untersuchung nach Zeitplan ist standardmäßig deaktiviert.

Um eine Untersuchung nach Zeitplan einzurichten, machen Sie Folgendes:

Auf der Registerkarte **Untersuchung** gehen Sie auf den Punkt **Zeitplan** und richten die Suchparameter ein (s. Abb. 37):

- **Täglich** – Untersuchung erfolgt jeden Tag. Die Untersuchungszeit wird mit dem Parameter **Startzeit** angegeben.
- **Wöchentlich** – Untersuchung erfolgt einmal pro Woche. Der Tag und die Uhrzeit für die Untersuchung werden mit den Parametern **Wochentag** und **Startzeit** bestimmt.
- **Deaktivieren** – Es erfolgt keine zeitgesteuerte Untersuchung.

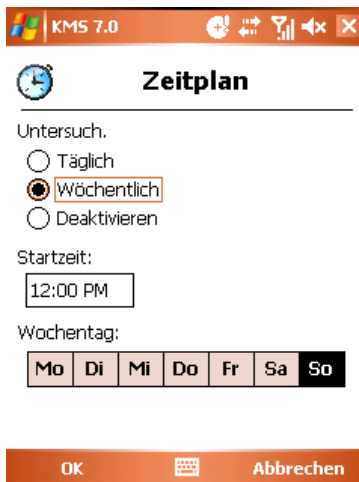


Abbildung 37. Menü **Zeitplan**

3.4. Isolieren in Quarantäne

Infizierte Objekte, die in die Quarantäne verschoben worden sind, bedrohen nicht mehr die Sicherheit Ihres mobilen Gerätes und können später gelöscht oder wiederhergestellt werden.

Als infiziert erkannte Objekte können von einer Anwendung entweder automatisch oder nach Ihrer expliziten Bestätigung in die Quarantäne verschoben werden.

Damit die Anwendung bei einer Viren-Suche automatisch infizierte Objekte in die Quarantäne verschiebt, wechseln Sie zur Registerkarte **Untersuchung**, wählen den Punkt **Scaneinstellungen** und setzen im Block **Bei Viruserkennung** die Option **Wenn Desinfektion nicht geht** auf den Wert **In Quarantäne**. Für den Fall, dass ein infiziertes Objekt nicht desinfiziert werden kann, setzen Sie zusätzlich ein Häkchen bei **Desinfektionsversuch** und gehen Sie in der Liste **Wenn Desinfektion nicht geht** auf **In Quarantäne**.

Wenn Sie **Aktion erfragen** angegeben haben, schlägt Ihnen Kaspersky Mobile Security beim Erkennen eines infizierten Objektes vor, das Objekt zu löschen oder es in die Quarantäne zu verschieben.

Den Inhalt der Quarantäne zeigen Sie an, indem Sie zur Registerkarte **Quarantäne** wechseln (s. Abb. 38).

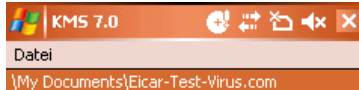


Abbildung 38. Quarantäne

Im **Menü**, das im Quarantäne-Fenster angeboten wird, können Sie Folgendes machen:

- Detaillierte Informationen zu einem markierten Objekt anzeigen, das in der Quarantäne gespeichert wird (Punkt **Hinweise**)
- Aktuelles Objekt löschen (Punkt **Löschen**)
- Aktuelles Objekt aus der Quarantäne in ursprüngliches Verzeichnis wiederherstellen (Punkt **Wiederherstellen**)
- Quarantäne leeren, indem der gesamte Inhalt mit den Objekten gelöscht wird (Punkt **Alle löschen**)

3.5. Module Anti-Spam und Diebstahlschutz (Anti-Theft)

Das Modul Anti-Spam schützt das Smartphone vor unerwünschten SMS- und MMS-Nachrichten.

Das Modul Anti-Theft sperrt das Smartphone und löscht bei einem Diebstahl oder Verlust des Gerätes Daten im Speicher.

3.5.1. Anti-Spam

Das Modul Anti-Spam schützt das mobile Gerät vor unerwünschten SMS-Nachrichten.

Das Filter-Prinzip für Nachrichten beruht auf der Verwendung einer so genannten „schwarzen“ und „weißen“ Liste. Nachrichten, die von Telefonnummern eingehen, die auf einer „Schwarzen“ Liste stehen, werden von Anti-Spam gesperrt. Nachrichten von Telefonnummern, die auf einer „weißen“ Liste stehen, werden nicht gesperrt.

Um die Parameter für Anti-Spam zu ändern, machen Sie Folgendes:

- 1 Gehen Sie auf der Registerkarte **Anti-Spam** auf den Menüpunkt **Einstellungen**.
- 2 Aktivieren / Deaktivieren Sie Anti-Spam, indem Sie das Häkchen in **Anti-Spam aktivieren** setzen oder entfernen.
- 3 Geben Sie an, ob der Empfang von SMS-Nachrichten von Nummern zugelassen werden soll, die in keiner Liste stehen. Entfernen oder setzen Sie das Häkchen bei **SMS immer annehmen von: unbekanntem Nummern**.

- 4 Geben Sie an, ob der Empfang von SMS-Nachrichten generell zugelassen werden soll, wenn die Nummer des Absenders in der Kontaktliste steht. Entfernen oder setzen Sie dazu das Häkchen bei **SMS immer annehmen von: Nummern in Kontaktliste**.

3.5.2. „Schwarze“ und „Weiße“ Liste bearbeiten

Die „Schwarze“ Liste enthält Telefonnummern, von denen der Empfang von Nachrichten durch Anti-Spam gesperrt wird.

Die „Weiße“ Liste enthält Telefonnummern, von denen der Empfang von Nachrichten zugelassen ist.

Um die „schwarze“ oder „weiße“ Liste zu bearbeiten, wechseln Sie auf die Registerkarte **Anti-Spam** (s. Abb. 39) und gehen Sie auf die entsprechende Liste.

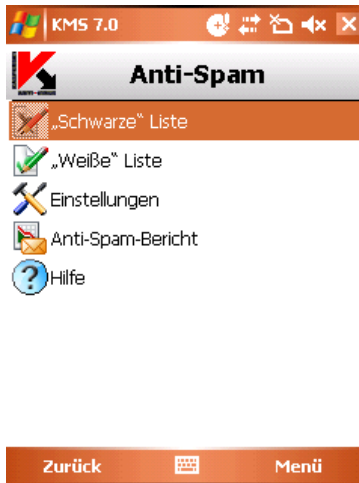
Zur Bearbeitung der Liste gehen Sie auf **Menü**:

- **Eintrag hinzufügen** – Es wird ein neuer Eintrag in der Liste erzeugt.
- **Eintrag löschen** – Der aktuelle Eintrag wird gelöscht.
- **Eintrag bearbeiten** – In der Liste wird der aktuelle Eintrag bearbeitet.

Nachdem Sie den Punkt **Eintrag hinzufügen** ausgewählt haben, geben Sie die Telefonnummer ein (Feld **Telefonnummer**), die Sie in die Liste aufnehmen wollen. Die Nummer kann mit einer Ziffer oder dem Zeichen „+“ beginnen. Außerdem dürfen beim Anlegen der Nummer die Ersatzzeichen „?“ (steht für eine einzelne Ziffer) und „*“ (steht für eine beliebig lange Ziffernfolge) verwendet werden.

Zusätzlich tragen Sie einen Text ein (Feld **Text**), bei dessen Erkennen durch das Programm in der eingegangenen Nachricht die folgenden Aktionen ausgeführt werden:

- Nachrichten, in denen Text gefunden wird, der in der "weißen" Liste steht, werden nicht ausgefiltert.
- Nachrichten, in denen Text gefunden wird, der in der "schwarzen" Liste steht, werden gesperrt.

Abbildung 39. Menü **Anti-Spam**

Die Analyse der Nachricht erfolgt in dieser Reihenfolge:

- Untersuchung der Nummer auf Zugehörigkeit zur "schwarzen" Liste
- Untersuchung der Nummer auf Zugehörigkeit zur "weißen" Liste
- Untersuchung des Nachrichtentextes danach, was in der "schwarzen" Liste steht
- Untersuchung des Nachrichtentextes danach, was in der "weißen" Liste steht

Wenn die Nachricht zu einer Regel passt, erfolgt die weitere Untersuchung, und die Nachricht wird übersprungen oder gesperrt, je nach der Zugehörigkeit zur "schwarzen" oder "weißen" Liste.

Zum Bearbeiten der Listen klicken Sie auf **OK**, um so zur Registerkarte **Anti-Spam** zurückzukehren.

3.5.3. Aktionen für Nachrichten

Geht eine Nachricht von einer Telefonnummer ein, die nicht in der „schwarzen“ oder „weißen“ Liste steht, erscheint im Display des mobilen Gerätes eine Warnmeldung (s. Abb. 40) – vorausgesetzt, dass in den Anti-Spam-Einstellungen der Nachrichten-Empfang von unbekannt Nummern zugelassen ist (s. Abb. 3.5.1 auf S. 44),



Abbildung 40. Anti-Spam warnt

Über den Punkt **Menü** können Sie eine der folgenden Aktionen für eine Nachricht wählen:

- In **„weiße“ Liste** – Der Empfang der Nachricht wird zugelassen, und die Telefonnummer des Absenders wird in die „weiße“ Liste gespeichert.
- In **„schwarze“ Liste** – Der Empfang der Nachricht wird gesperrt, und die Telefonnummer des Absenders wird in die „schwarze“ Liste gespeichert.

Klicken Sie auf **Überspr.**, um den Empfang der Nachricht zuzulassen. Die Telefonnummer des Absenders wird dann in keine Liste gespeichert.

Die Daten über gesperrte Nachrichten werden in das Anwendungsprotokoll eingetragen. Um dieses Protokoll anzuzeigen, klicken Sie auf der Registerkarte **Anti-Spam** auf **Bericht**, oder Sie gehen auf der gleichen Registerkarte auf den Punkt **Anti-Spam-Bericht**. Außerdem erreichen Sie den Bericht auf der Registerkarte **Hinweis** (s. Pkt. 3.8 auf S. 54).

3.5.4. Diebstahlschutz (Anti-Theft)

Das Modul Diebstahlschutz (Registerkarte **Sonstiges**, Punkt **Diebstahlschutz** (s. Abb. 41) schützt Daten, die auf dem mobilen Gerät gespeichert sind, vor dem unautorisierten Zugriff, falls das Gerät gestohlen wird oder verloren geht.

Beim erstmaligen Aufruf der Modul-Einstellungen muss ein Geheimcode definiert werden. Mit dessen Hilfe können Sie künftig auf die Modul-Einstellungen zugreifen, um sie zu ändern. Der Geheimcode wird gebraucht, damit die Einstellungen nicht unautorisiert geändert werden können und damit der Benutzer Daten sperren und löschen kann, die auf dem Smartphone Gerät bei Diebstahl oder Verlust gespeichert waren.

Die Funktion **SMS-Block** sperrt das Gerät auf Wunsch des Benutzers. Es lässt sich erst nach Eingabe eines Geheimcodes entsperren, der für den Zugriff auf das Diebstahlschutz-Modul verwendet wird. Die Einstellung tritt in Kraft, nachdem der Benutzer, dem das Smartphone gestohlen wurde, an das gestohlene Gerät die SMS **block:Code** (also **block:** direkt gefolgt von dem entsprechenden Code) sendet. Die Funktion **SMS-Block** wird bei deren Auswahl aktiviert: Lesen Sie die Informationsnachricht und klicken Sie auf **OK**, wenn Sie diese Option nutzen wollen.

Die Funktion **SMS-Clean** löscht persönliche Benutzerdaten (Kontakte, Posteingang, persönliche Dateien). Die Einstellung tritt in Kraft, nachdem der Benutzer, dem das Gerät gestohlen wurde, an das gestohlene Gerät die SMS **clean:Code** (also **clean:** (also „block:“, direkt gefolgt von dem entsprechenden Code) direkt gefolgt von dem entsprechenden Code) sendet. Die Funktion **SMS-Clean** wird bei deren Auswahl aktiviert: Geben Sie die gewünschten Einstellungen an (s. Pkt. 3.5.4.1 auf S. 49), lesen Sie die Informationsnachricht und klicken Sie auf **OK**, wenn Sie diese Option nutzen wollen.

Die Funktion **SIM-Watch** sendet beim Wechsel der SIM-Karte auf einem gestohlenen Smartphone die Telefonnummer der neuen Karte an die hinterlegten Nummern und sperrt das Gerät. Das Gerät wird mit Eingabe des Geheimcodes entsperrt, der für den Zugriff auf das Diebstahlschutz-Modul angegeben wurde. Die Funktion SIM-Watch wird bei deren Auswahl aktiviert: Geben Sie die gewünschten Einstellungen an (s. Pkt. 3.5.4.2 auf S. 50), lesen Sie die Informationsnachricht und klicken Sie auf **OK**, wenn Sie diese Option nutzen wollen.

Wenn der Geheimcode für das Diebstahlschutz-Modul geändert werden muss, gehen Sie auf den Punkt **Code ändern**. Geben Sie den neuen Code ein, wiederholen ihn zur Sicherheit nochmal und klicken Sie auf **OK**.

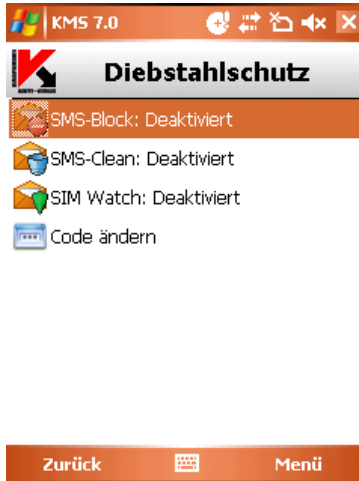


Abbildung 41. Registerkarte **Diebstahlschutz**

Die vorgenommenen Aktionen werden in das Anwendungsprotokoll eingetragen. Um das Protokoll anzuzeigen, gehen Sie auf der Registerkarte **Sonstiges** auf den Punkt **Diebstahlschutz-Bericht**. Außerdem erreichen Sie den Bericht auf der Registerkarte **Informationen** (s. Pkt. 3.8 auf S. 54).

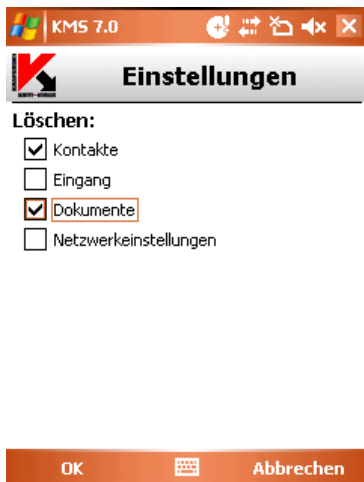
3.5.4.1. Konfiguration von SMS-Clean

Der Abschnitt **SMS-Clean** enthält eine Liste von Daten, die für den Fall gelöscht werden, wenn das Smartphone gestohlen wird oder verloren geht (s. Abb. 42).

Um die Parameter für SMS-Clean zu ändern, führen Sie die folgenden Aktionen aus:

- .1 Wählen Sie auf der Registerkarte **Sonstiges** den Punkt **Diebstahlschutz**.
- .2 Geben Sie den Geheimcode ein und gehen Sie im nächsten Fenster auf den Punkt **SMS-Clean**.
- .3 Setzen Sie das Häkchen bei **Kontakte**, wenn Sie möchten, dass bei einem Verlust oder Diebstahl des mobilen Gerätes das Telefonbuch gelöscht wird.
- .4 Setzen Sie das Häkchen bei **Eingang**, wenn Sie wollen, dass die Post sowie die SMS- und MMS-Nachrichten gelöscht werden.
- .5 Setzen Sie das Häkchen bei **Dokumente**, wenn die persönlichen Benutzerdaten gelöscht werden sollen.

- .6 Setzen Sie das Häkchen bei **Netzwerkeinstellungen**, wenn die Netzwerkeinstellungen gelöscht werden sollen.
- .7 Klicken Sie auf **OK**, um die vorgenommenen Einstellungen zu speichern.

Abbildung 42. Registerkarte **SMS-Clean**

3.5.4.2. Konfiguration von SIM-Watch

Der Abschnitt **SIM Watch** überwacht den Wechsel der SIM-Karte auf dem Gerät (s. Abb. 43).

Um die Parameter für SIM Watch zu ändern, führen Sie die folgenden Aktionen aus:

- .1 Auf der Registerkarte **Sonstiges** gehen Sie auf den Punkt **Diebstahlschutz**.
- .2 Geben Sie den Geheimcode ein und gehen Sie im nächsten Fenster auf den Punkt **SIM-Watch**.
- .3 In den Feldern **1)** und **2)** geben Sie diejenigen Telefonnummern ein, an die Sie die neue Telefonnummer erhalten wollen, falls die SIM-Karte auf Ihrem Smartphone gewechselt wird. Die Nummern können mit einer Ziffer oder dem Zeichen „+“ beginnen und dürfen nur Ziffern enthalten.
- .4 Richten Sie die Sperre des mobilen Gerätes beim Wechsel der SIM-Karte ein. Aktivieren Sie dazu das entsprechende Kontrollkästchen **Sperren**.

- .5 Klicken Sie auf **OK**, um die eingegebenen Daten zu speichern.



KMS 7.0

Telefonnummern

1) 89991234567

2) +70001234567

Sperren

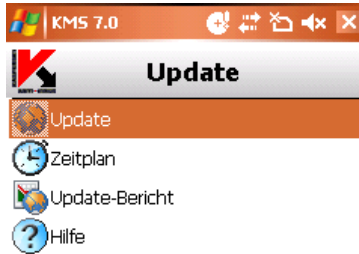
OK Abbrechen

Abbildung 43. Registerkarte **SIM-Watch**

3.6. Update der Programm-Datenbanken

Nach schädlichen Programmen wird mit Hilfe von Einträgen in der Datenbank von Kaspersky Mobile Security gesucht, in der eine Beschreibung aller bekannten und zur Zeit als schädlich eingestuften Programme steht. Es ist absolut wichtig, dass die Datenbanken stets auf dem neuesten Stand sind.

Die Datenbanken können entweder manuell oder nach Zeitplan aktualisiert werden. Zum Einrichten und Starten eines Updates dient die Registerkarte **Update** (s. Abb. 44). Das Update erfolgt über das Internet von den Kaspersky-Lab-Servern. Tritt ein Fehler auf, schauen Sie bitte nach, ob das mobile Gerät Zugriff auf das Internet hat.

Abbildung 44. Registerkarte **Update**

Der Update-Vorgang der Datenbanken wird in das Protokoll eingetragen. Um dieses Protokoll anzuzeigen, gehen Sie auf der Registerkarte **Update** auf den Punkt **Updatebericht**. Außerdem erreichen Sie den Bericht auf der Registerkarte **Informationen** (s. Pkt. 3.8 auf S. 54).

Um manuell das Update der Programm-Datenbanken von den Update-Servern bei Kaspersky Lab zu starten, machen Sie Folgendes:

- .1 Starten Sie Kaspersky Mobile Security (s. Pkt. 3.2.1 auf S. 34) und wechseln Sie zur Registerkarte **Update**.
- .2 Gehen Sie auf **Update**, um den Update-Download zu starten.

Um einen Zeitplan für das automatische Update der Programm-Datenbanken einzurichten, machen Sie Folgendes:

- .1 Starten Sie Kaspersky Mobile Security (s. Pkt. 3.2.1 auf S. 34) und wechseln Sie zur Registerkarte **Update**.
- .2 Wählen Sie **Zeitplan** aus, um einen Zeitplan für automatische Updates einzurichten.
- .3 Geben Sie das Update-Intervall als Wert für den Update-Parameter ein:
 - **Täglich** – Updates erfolgen jeden Tag. Geben Sie zusätzlich die **Startzeit** des Updates vor.
 - **Wöchentlich** – Updates erfolgen einmal pro Woche. Geben Sie zusätzlich den **Wochentag** und die **Startzeit** des Updates ein.

- **Deaktivieren** – Updates müssen manuell durchgeführt werden.

Auf der Registerkarte **Informationen** können Sie das Erstellungsdatum für die Anti-Virus-Datenbanken erfahren, die in Ihrem mobilen Gerät installiert sind, sowie die Summe der Virussignaturen. Gehen Sie dazu auf der Registerkarte auf den Punkt **Infos zu Datenbanken**.

3.7. Firewall

Die **Firewall** kontrolliert die Netzwerkaktivität und den Schutz des mobilen Gerätes auf Netzwerkebene (s. Abb. 45).

Um die Parameter für die Firewall zu ändern, führen Sie die folgenden Aktionen aus:

- .1 Starten Sie Kaspersky Mobile Security (s. Pkt. 3.2.1 auf S. 34) und wechseln Sie zur Registerkarte **Firewall**.
- .2 Gehen Sie auf den Punkt **Firewall-Einstellungen**. Im nächsten Fenster können Sie die Schutzstufe einrichten, um eine Überwachungsstufe für den ein- und ausgehenden Traffic festzulegen. Es gibt die folgenden Varianten:
 - **Alle blockieren** - Jede Netzwerkaktivität wird unterbunden.
 - **Mittel** - Der eingehende Traffic wird gesperrt. Ausgehende Verbindungen können nur über die Standard-Anwendungen erfolgen.
 - **Niedrig** - Es werden nur eingehende Verbindungen gesperrt.
 - **Deaktiviert** - Der Netzwerkaktivität wird zugelassen.

Die Ereignisse des Firewall-Moduls werden in das Protokoll eingetragen. Um dieses Protokoll anzuzeigen, gehen Sie auf der Registerkarte **Firewall** auf den Punkt **Firewall-Bericht**. Außerdem erreichen Sie den Bericht auf der Registerkarte **Informationen** (s. Pkt. 3.8 auf S. 54).

Abbildung 45. Registerkarte **Firewall**

3.8. Ereignisprotokoll

Das Ereignisprotokoll sehen Sie auf der Registerkarte **Informationen** unter dem Punkt **Berichte** ein. Sie können einen Bericht für eine beliebige Aufgabe anzeigen, die Kaspersky Mobile Security ausgeführt hat:

- Untersuchungsbericht
- Update-Bericht
- Firewall-Bericht
- Anti-Spam-Bericht
- Diebstahlschutz -Bericht

Um beispielsweise einen Bericht über eine Viren-Suche anzusehen, machen Sie Folgendes:

- .1 Starten Sie Kaspersky Mobile Security (s. Pkt. 3.2.1 auf S. 34).
- .2 Auf der Registerkarte **Informationen** gehen Sie auf den Punkt **Berichte** (s. Abb. 46).
- .3 Im nächsten Fenster wählen Sie **Untersuchungsbericht**.

Abbildung 46. Registerkarte **Berichte**

3.9. Deinstallation der Anwendung

Um Kaspersky Mobile Security zu deinstallieren, machen Sie Folgendes:

1. Deaktivieren Sie den Echtzeitschutz (Details s. Pkt. 3.3 auf S. 38).

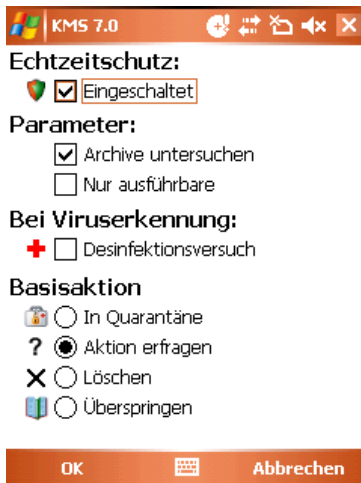


Abbildung 47. Echtzeitschutz deaktivieren

2. Beenden Sie Kaspersky Mobile Security. Gehen Sie dazu im Programmmenü auf den Punkt **Beenden** (s. Abb. 48).



Abbildung 48. Programm beenden

3. Deinstallieren Sie die Anwendung. Machen Sie dazu Folgendes:
 - Klicken Sie auf die Schaltfläche **Start**, gehen Sie auf das Menü **Einstellungen** und dann auf **Programm entfernen**. Falls Sie eine englischsprachige Version von Windows Mobile verwenden, wählen Sie analog dazu die Menüpunkte **System** und **Remove Programs** (s. Abb. 49):

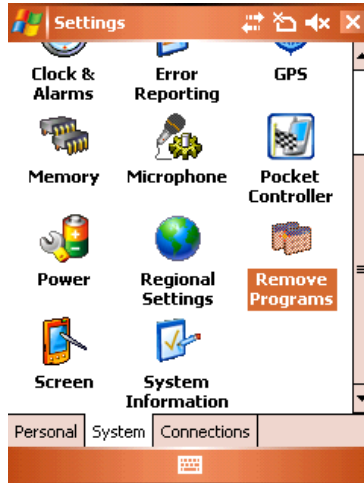


Abbildung 49. Programm-Deinstallation

- In der Liste der installierten Programme gehen Sie auf **Kaspersky Mobile Security** und klicken auf die Schaltfläche **Deinstallieren** (s. Abb. 50).

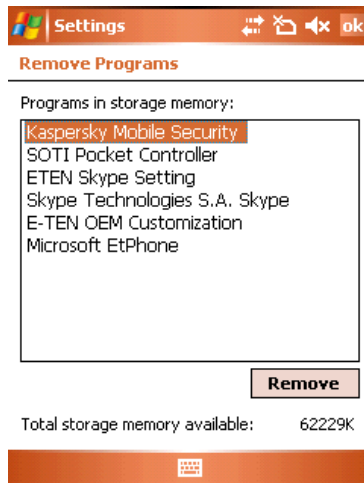


Abbildung 50. Programm auswählen

- Bei der Bestätigungsabfrage für die Programm-Deinstallation klicken Sie auf die Schaltfläche **Ja** (s. Abb. 51).

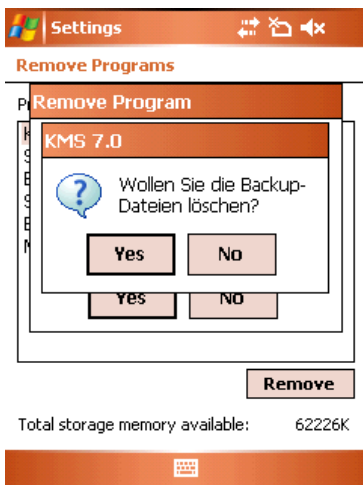


Abbildung 51. Bestätigungsabfrage für Programm-Deinstallation

ANHANG A. KASPERSKY LAB

Das Unternehmen

Kaspersky Lab ist ein weltweit führendes Unternehmen in den Bereichen Viren-, Spam- und Hacker-Schutz. Unser hoch spezialisiertes Viren-Labor reagiert stets schneller als alle anderen auf neue Bedrohungen, so dass unsere innovativen Programme seit vielen Jahren Heimanwender und Unternehmen jeder Größe zuverlässig schützen.

Bereits 1997 wurde Kaspersky Lab von dem russischen Virenexperten Eugene Kaspersky in Moskau gegründet und hat heute unter anderem Niederlassungen in Deutschland, Frankreich, Großbritannien, Polen, Japan, USA und China.

Einzigartige Erfahrung

Weltweit beschäftigt Kaspersky Lab über 1.000 hochspezialisierte Mitarbeiter, darunter Mitglieder der Computer Anti-Virus Researchers Organisation (CARO) und des Virus Bulletin Technical Advisory Board. Im Laufe vieler Jahre Forschung und Kampf gegen Computerviren haben wir Wissen und Fähigkeiten erworben, die heute unser wertvollstes Kapital darstellen.

Dank unserer weit reichenden Erfahrung sind wir in der Lage, Entwicklungstrends bei Malware vorherzusehen. Dieser einzigartige Vorteil bildet die Basis der Produkte und Dienstleistungen von Kaspersky Lab, so dass wir anderen immer einen Schritt voraus sind und unseren Kunden stets den besten Schutz bieten können.

Kaspersky Anti-Virus

Nach vielen Jahren innovativer Entwicklungen zählt Kaspersky Lab heute zu den führenden Herstellern von Sicherheits-Software. Der hohe Standard unserer Produkte wird durch zahlreiche Auszeichnungen internationaler Forschungseinrichtungen, unabhängiger Testlabors und renommierter Fachpublikationen bestätigt.

Die Programm-Module unseres bekanntesten Programms, Kaspersky Anti-Virus, gewährleisten einen zuverlässigen Schutz für Workstations, Datei- und Web-Server, Mail-Gateways, Firewalls, Pocket-PCs und Smartphones.

Als erstes Unternehmen entwickelte Kaspersky Lab bedeutende Technologien, die heute selbst bei zahlreichen Antiviren-Programmen anderer Hersteller als Programm-Kern einen unverzichtbaren Bestandteil bilden. So vertrauen bereits über 200 Millionen Anwender unseren Innovationen, wie dem heuristischen Analysator zur Entdeckung noch unbekannter Viren, den Micro-Updates für die Antiviren-Datenbanken und dem ersten umfassenden Virenschutz für Unix/Linux-Systeme.

Komplexe Technologien für Ihre Sicherheit

Moderne Viren und Schadprogramme sind komplexe Bedrohungen, so dass die bisher üblichen Schutzpakete für PCs und Netzwerke häufig nicht mehr ausreichen.

Aus diesem Grund entwickelte Kaspersky Lab mit Kaspersky Anti-Hacker eine Personal Firewall und mit Kaspersky Anti-Spam einen besonders effektiven Spam-Filter. Mit den Produkten von Kaspersky Lab können Sie Ihren Computer und Ihr Netzwerk optimal vor allen modernen virtuellen Gefahren schützen.

Service

Kaspersky Lab bietet seinen Kunden eine ganze Palette zusätzlicher Dienstleistungen, die einen maximalen Schutz garantieren: Die Antiviren-Datenbanken werden stündlich aktualisiert, die Anti-Spam-Dateien 12 bis 24 Mal pro Tag. Zudem steht allen Anwendern ein Rund-um-die-Uhr-Support zur Verfügung: Telefonisch oder per E-Mail – in deutscher, englischer, russischer und französischer Sprache.

A.1. Kontaktinformationen

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir werden Sie gern umfassend per Telefon oder E-Mail beraten.

Weitere Information erhalten Sie bei:

Kaspersky Labs GmbH
Steinheilstraße 13
85053 Ingolstadt

Technischer Support	Tel.: +49 (0)180 555 46 24 (14 Cent/Minute aus dem deutschen Festnetz) E-Mail: kavmobile@kaspersky.de
Allgemeine Informationen	WWW: www.kaspersky.de www.viruslist.de
Feedback zu unseren Benutzerhandbüchern	docfeedback@kaspersky.de (Diese Adresse ist ausschließlich für Rückmeldungen über das Handbuch und elektronische Hilfesystem gedacht.)

ANHANG B. ENDBENUTZER- LIZENZVERTRAG FÜR DIE ERWORBENE KASPERSKY LAB SOFTWARE

WICHTIG - bitte sorgfältig lesen: Lesen Sie die in diesem KASPERSKY LAB Endbenutzer-Lizenzvertrag ("EULA") beschriebenen Rechte und Einschränkungen sorgfältig durch. Sie werden gebeten, die Bestimmungen des EULAs zu prüfen und ihnen zuzustimmen oder diese abzulehnen.

Indem Sie das Sicherheitsetikett auf der CD/DVD-Box aufreißen oder wenn Sie die SOFTWARE installieren, erklären Sie sich mit den Bestimmungen des EULAs einverstanden. Falls Sie mit den Bestimmungen des EULAs NICHT einverstanden sind, geben Sie die erworbene Software bitte innerhalb von 14 Tagen an die Einkaufsstelle zurück. Nach Eingabe des Aktivierungscode ist eine Rückgabe der Software ausgeschlossen.

Jede Bezugnahme auf "Software" schließt den Aktivierungscode oder die Schlüsseldatei ein, den Sie von Kaspersky Lab als Teil der Software erhalten.

Dieser EULA ist ein rechtsgültiger Vertrag zwischen Ihnen, dem Besitzer eines Exemplars der SOFTWARE (entweder als natürlicher oder als juristischer Person) und KASPERSKY LAB. KASPERSKY LAB wird sich das exklusive Urheberrecht auf die Computersoftware (auf die Software und die Antiviren-Datenbanken) vorbehalten. Indem Sie die SOFTWARE installieren, erklären Sie sich damit einverstanden, durch die Bestimmungen dieses EULAs gebunden zu sein. Falls Sie den Bestimmungen dieses EULAs nicht zustimmen, sind Sie nicht berechtigt, die SOFTWARE zu installieren und zu verwenden.

Die SOFTWARE ist sowohl durch Urheberrechtsgesetze und internationale Urheberrechtsverträge als auch durch andere Gesetze und Vereinbarungen über geistiges Eigentum geschützt.

1. LIZENZEINRÄUMUNG. Durch diesen EULA werden Ihnen folgende Rechte eingeräumt:

- Sie sind berechtigt, eine Kopie der SOFTWARE auf einem einzigen Computer zu installieren und zu verwenden. Eine Mehrplatzlizenz der SOFTWARE, dürfen Sie auf so vielen Computern installieren, wie Sie Lizenzen erworben haben.
- Sie sind berechtigt, die installierte SOFTWARE gemäß den Bestimmungen dieses Vertrags zu benutzen. Das Recht, Aktualisierungen (Updates) der SOFTWARE zu beziehen, besteht nur, wenn sie es mit

dem Verkäufer der SOFTWARE vereinbart haben und nur für die vereinbarte Dauer. Wenn Sie aufgrund Kaufvertrags oder in sonstiger Weise berechtigt sind, Aktualisierungen zu beziehen, so gelten die Bestimmungen dieses Vertrags entsprechend für die aktualisierte SOFTWARE. Sie können diesen Vertrag jederzeit kündigen, indem Sie alle Kopien der Software und der Dokumentation zerstören.

2. EINSCHRÄNKUNGEN

- Einschränkungen im Hinblick auf Zurückentwicklung (Reverse Engineering), Dekompilierung und Disassemblierung. Sie sind nicht berechtigt, die SOFTWARE zurückzuentwickeln (Reverse Engineering), zu dekompileieren oder zu disassemblieren, es sei denn und nur insoweit, wie das anwendbare Recht, ungeachtet dieser Einschränkung, dies ausdrücklich gestattet. Sie sind nicht berechtigt, diese Software in automatischen, halbautomatischen oder manuellen Tools zu verwenden, welche dazu dienen, Virensignaturen, Virenerkennungsroutinen, sowie beliebige andere Daten oder Codes zum Erkennen von schädlichem Code oder Daten zu erstellen.
- Vermietung. Sie sind nicht berechtigt, die SOFTWARE zu vermieten, zu verleasen oder zu verleihen.
- Supportleistungen. Nach Kauf und Aktivierung der SOFTWARE erhalten Sie sofort das Recht auf die Supportleistungen für die beim Kauf der SOFTWARE oder unabhängig davon vereinbarte Dauer. Supportleistungen verstehen sich wie folgt:
 - stündliche Updates der Antiviren-Datenbank
 - kostenloses Updates der Software
 - technische Unterstützung sowohl per e-Mail als auch per Telefon mit KASPERSKY LAB

3. KÜNDIGUNG. Unbeschadet sonstiger Rechte ist KASPERSKY LAB berechtigt, diesen EULA fristlos zu kündigen, sofern Sie gegen die Bestimmungen dieses EULAs verstoßen. In einem solchen Fall sind Sie verpflichtet, sämtliche Kopien der SOFTWARE und alle ihre Komponenten zu vernichten.

4. URHEBERRECHT. Das Urheberrecht auf die Software, die gedruckten Begleitmaterialien und jede Kopie der Software liegt bei Kaspersky Lab, soweit es durch die Veräußerung nicht erschöpft ist.

5. GEWÄHRLEISTUNG. Kaufvertragliche Gewährleistungsansprüche bestehen nur gegenüber dem Unternehmen oder der Person, von der Sie die Software gekauft haben. Mit diesem Lizenzvertrag ist keine Erweiterung der kaufrechtlichen Gewährleistung verbunden. Nur für den Fall, dass Sie die Software unmittelbar von Kaspersky Lab gekauft haben sollten, gilt: KASPERSKY LAB gewährleistet, dass:

- die SOFTWARE den Spezifikationen im Wesentlichen entspricht.

- im Falle einer physikalischen Lieferung der Originaldatenträger frei von Material- und Herstellungsfehlern ist.
- das Programm korrekt auf den Datenträger aufgezeichnet ist, die Dokumentation sämtliche Informationen enthält, die KASPERSKY LAB für die Benutzung der Software für erforderlich hält.
- die SOFTWARE binnen 90 Tagen ab der ersten Installation oder dem ersten Download, falls richtig behandelt, der in der beiliegenden Dokumentation bestimmten Funktionalität entspricht und laut derer voll funktionsfähig ist.

Gewährleistungspflichtige Mängel werden von KASPERSKY LAB oder dessen Lieferanten nach Entdeckung, auf jeden Fall aber vor Ablauf von der Gewährleistungsfrist, dem Ermessen von Kaspersky Lab nach, durch Ersatz, Reparatur, Umtausch oder Rückzahlung beseitigt, falls eine Mängelrüge rechtzeitig an Kaspersky Lab oder dessen Lieferanten gerichtet wurde. KASPERSKY LAB oder dessen Lieferanten übernehmen keine Gewährleistung für Mängel, die auf andere als für die Software vorgesehenen Einsatzbedingungen, unsachgemäße Behandlung oder dergleichen zurückzuführen sind.

ALLE ANDERE GEWÄHRLEISTUNGEN UND BEDINGUNGEN, SEIEN SIE AUSDRÜCKLICH ODER KONKLUDENT, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF, (FALLS ZUTREFFEND) JEDE KONKLUDENTE GEWÄHRLEISTUNG IM HINBLICK AUF HANDELSÜBLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, FAHRLÄSSIGKEIT ODER MANGELNDE FACHMÄNNISCHE BEMÜHUNGEN WERDEN VON KASPERSKY LAB ODER DESSEN LIEFERANTEN ABGELEHNT. ES BESTEHT EBENFALLS KEINE GEWÄHRLEISTUNG ODER BEDINGUNG VON RECHTSANSPRÜCHEN IN BEZUG AUF RECHTSINHABERSCHAFT, UNGESTÖRTES NUTZUNGSVERGNÜGEN ODER NICHTVERLETZUNG VON RECHTEN DRITTER. DAS GESAMTE RISIKO, DAS BEI DER BENUTZUNG ODER LEISTUNG DER SOFTWARE ENTSTEHT, LIEGT BEI IHNEN.

6. AUSSCHLUSS DER HAFTUNG FÜR ALLE SCHÄDEN. SOWEIT GESETZLICH ZUGELASSEN, SIND KASPERSKY LAB ODER DESSEN LIEFERANTEN IN KEINEM FALL HAFTBAR FÜR IRGENDWELCHE FOLGE-, ZUFÄLLIGEN, DIREKTEN, INDIREKTEN, SPEZIELLEN, STRAFRECHTLICHEN ODER ANDEREN SCHÄDEN WELCHER ART AUCH IMMER (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SCHÄDEN AN PERSONEN ODER SACHEN, SCHÄDEN AUS ENTGANGENEM GEWINN, GESCHÄFTSUNTERBRECHUNG, VERLUST VON GESCHÄFTLICHEN INFORMATIONEN, FÜR DEN VERLUST VON PRIVATSPHÄRE, DIE UNMÖGLICHKEIT, EINE PFLICHT ZU ERFÜLLEN (EINSCHLIESSLICH GEMÄSS TREU UND GUTEN GLAUBENS ODER VERNÜNFTIGER ANGEMESSENER SORGFALT) ZU ERFÜLLEN, FÜR FAHRLÄSSIGKEIT ODER ANDERE VERMÖGENSSCHÄDEN), DIE AUS DER VERWENDUNG DER SOFTWARE ODER DER TATSACHE, DASS SIE NICHT VERWENDET

WERDEN KANN, RESULTIEREN ODER DAMIT IN ZUSAMMENHANG STEHEN, SELBST WENN KASPERSKY LAB ODER DESSEN LIEFERANTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WORDEN IST. DIESER HAFTUNGS AUSSCHLUSS FÜR SCHÄDEN GILT AUCH DANN, WENN ABHILFEMASSNAHMEN IHREN WESENTLICHEN ZWECK VERFEHLEN.

7. ANWENDBARES RECHT. Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland. Die Geltung des UN-Kaufrechts ist ausgeschlossen.